신뢰할 수 있는 발신자를 화이트리스트에 추가하려면 어떻게 해야 합니까?

목차

질문

신뢰할 수 있는 발신자를 화이트리스트에 추가하려면 어떻게 해야 합니까?

응답

이 발신자 그룹은 $TRUSTED 메일 플로우 정책을 사용하므로 Cisco ESA(Email Security Appliance)에서 신뢰하는 발신자를 WHITELIST 발신자 그룹에 추가합니다.WHITELIST 발신자 그룹의 구성원은 속도 제한의 대상이 아니며, 이러한 발신자의 콘텐츠는 Cisco IronPort AntiSpam 엔진에서 검사되지 않지만 Sophos Anti-Virus 소프트웨어에서 스캔됩니다.

> **참고**: 기본적으로 안티바이러스 검사가 활성화되지만 안티스팸은 꺼져 있습니다.

발신자를 화이트리스트에 추가하려면 HAT(Host Access Table)의 WHITELIST 발신자 그룹에 발신자를 추가합니다. GUI 또는 CLI를 통해 HAT를 구성할 수 있습니다.

GUI에서

1. *메일 정책* 탭을 클릭합니다.
2. *Host Access Table* 섹션에서 *HAT Overview*를 선택합니다.
3. 오른쪽에서 InboundMail *Listener*가 현재 선택되어 있는지 확인합니다.
4. 아래의 *Sender Group* 열에서 WHITELIST(화이트리스트)를 클릭합니다.
5. 페이지 하단의 *Add Sender*(발신자 추가) 버튼을 클릭합니다.
6. 첫 번째 필드에 화이트리스트에 추가할 IP 또는 호스트 이름을 입력합니다.

항목 추가를 완료하면 *Submit* 버튼을 클릭합니다.Commit Changes(변경 사항 *커밋)* 버튼을 클릭하여 변경 사항을 저장합니다.

CLI에서

```
example.com> listenerconfig
Currently configured listeners:
1. InboundMail (on PublicNet, 172.19.1.80) SMTP TCP Port 25 Public
2. OutboundMail (on PrivateNet, 172.19.2.80) SMTP TCP Port 25 Private
Choose the operation you want to perform:
- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.
[]> edit
Enter the name or number of the listener you wish to edit.
[]> 1
Name: InboundMail
Type: Public
Interface: PublicNet (172.19.1.80/24) TCP Port 25
Protocol: SMTP
Default Domain:
Max Concurrency: 1000 (TCP Queue: 50)
Domain Map: Disabled
TLS: No
SMTP Authentication: Disabled
Bounce Profile: Default
Use SenderBase For Reputation Filters and IP Profiling: Yes
Footer: None
LDAP: Off

Choose the operation you want to perform:
- NAME - Change the name of the listener.
- INTERFACE - Change the interface.
- LIMITS - Change the injection limits.
- SETUP - Configure general options.
- HOSTACCESS - Modify the Host Access Table.
- RCPTACCESS - Modify the Recipient Access Table.
- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this
listener.
- MASQUERADE - Configure the Domain Masquerading Table.
- DOMAINMAP - Configure domain mappings.
[]> hostaccess
Default Policy Parameters
==========================
Allow TLS Connections: No
Allow SMTP Authentication: No
Require TLS To Offer SMTP authentication: No
Maximum Concurrency Per IP: 1,000
Maximum Message Size: 100M
Maximum Messages Per Connection: 1,000
Maximum Recipients Per Message: 1,000
Maximum Recipients Per Hour: Disabled
Use SenderBase For Flow Control: Yes
Spam Detection Enabled: Yes
Virus Detection Enabled: Yes
There are currently 4 policies defined.
There are currently 5 sender groups.
Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- MOVE - Move an entry.
```

```
- DEFAULT - Set the defaults.
- PRINT - Display the table.
- IMPORT - Import a table from a file.
- EXPORT - Export the table to a file.
- CLEAR - Remove all entries.
[]> edit
1. Edit Sender Group
2. Edit Policy
[1]> 1
Currently configured HAT sender groups:
1. WHITELIST (My trusted senders have no Brightmail or rate limiting)
2. BLACKLIST (Spammers are rejected)
3. SUSPECTLIST (Suspicious senders are throttled)
4. UNKNOWNLIST (Reviewed but undecided, continue normal acceptance)
5. (no name, first host = ALL) (Everyone else)
Enter the sender group number or name you wish to edit.
[]> 1

Choose the operation you want to perform:
- NEW - Add a new host.
- DELETE - Remove a host.
- MOVE - Reorder the hosts.
- POLICY - Change the policy settings and options.
- PRINT - Display the current definition.
- RENAME - Rename this sender group.
[]> new
Enter the hosts to add. CIDR addresses such as 10.1.1.0/24 are allowed. IP
address ranges such as 10.1.1.10-20 are allowed. IP subnets such as 10.2.3. are
allowed. Hostnames such as crm.example.com are allowed. Partial hostnames such
as .example.com are allowed.
Ranges of SenderBase Reputation scores such as SBRS[7.5:10.0] are allowed.
SenderBase Network Owner IDs such as SBO:12345 are allowed.
Remote blacklist queries such as dnslist[query.blacklist.example] are allowed.
Separate multiple hosts with commas
[]>
```

다음 사항을 실행해야 합니다. `commit` 명령을 사용하여 변경 사항을 저장합니다.

관련 정보

- Cisco Email Security Appliance – 엔드 유저 가이드
- 기술 지원 및 문서 – Cisco Systems